

Pearson Higher Nationals in Computing

Unit 43: Internet of Things



Acknowledgement

The internship opportunity I had with BCAS campus was a great chance for learning and professional development. Therefore, I consider myself as a very lucky individual as I was provided with an opportunity to be a part of it. I am also grateful for having chance to meet so many wonderful people and professionals who led me through this internship period.

I express my deepest thanks to the assessor Mr. Mohamed Nizzad, who works as an IT professional and take lectures on computer programming related subjects and others supportive subjects. He helped me taking part in useful decision & giving necessary advices and guidance and arrange all facilities for this assignment. I choose this moment to acknowledge his contribution gratefully. I acknowledge that this assignment was done with help of internet resources.

Sincerely,

S. SHALOMSHAN

Date:30.12.2022

Introduction

The Internet of Things (IoT) refers to the connection of devices, such as appliances, vehicles, and other items embedded with sensors, electronics, and connectivity, to the internet. This allows these objects to collect and exchange data, enabling them to be controlled remotely and to perform a variety of tasks. The IoT has the potential to transform the way we live and work, by enabling a range of applications such as smart homes, smart cities, and industrial automation.

IoT devices communicate with each other and with servers through the internet, using a variety of communication technologies and protocols. Some common technologies used in the IoT include Bluetooth, Wi-Fi, and cellular networks. These devices often use sensors to collect data about their environment, which is then transmitted to a central server or cloud platform for processing and analysis.

One of the main benefits of the IoT is that it allows for automation and the remote control of devices, which can improve efficiency and convenience. For example, a smart thermostat can learn a user's schedule and automatically adjust the temperature of a home to save energy, and a smart irrigation system can monitor soil moisture and adjust watering schedules to conserve water.

However, the use of the IoT also raises concerns about security and privacy, as connected devices can potentially be hacked and used to access sensitive information or disrupt systems. It is important for organizations and individuals to consider the security implications of the IoT and take steps to protect their devices and data.

Contents

Internet of Things	1
Acknowledgement	2
Introduction.....	3
Part 1	5
Explore various form of IOT functionality and Review and List down in a chart about Standard architecture, Frameworks, Tools, Hardware and APIs available for use in IOT developments through an internet survey.	5
Part 2	8
As an internet survey report, Analyze the impact of common IoT architecture, frameworks, tools, hardware and APIs in the software development life cycle.....	8
Part 4	10
Make some researches to evaluate above example scenario's (ADAS – emergency break) IOT architecture and justify their use when designing software applications.....	10
Part 5	11
Conclusion	14
Reference	15

Part 1

Explore various form of IOT functionality and Review and List down in a chart about Standard architecture, Frameworks, Tools, Hardware and APIs available for use in IOT developments through an internet survey.

There are many different aspects to consider when developing an Internet of Things (IoT) system, including the standard architecture, frameworks, tools, hardware, and APIs that can be used.

Standard Architecture:

- **OSI Model:** The Open Systems Interconnection (OSI) model is a standard architecture that defines the various layers of communication protocols in a networked system. It is often used as a reference for designing and implementing IoT systems.
- **MQTT:** The MQTT (Message Queuing Telemetry Transport) protocol is a lightweight publish/subscribe messaging protocol that is widely used in IoT systems. It is designed for low-bandwidth, high-latency networks and is often used to connect devices to a central broker.
- **CoAP:** The Constrained Application Protocol (CoAP) is a lightweight protocol that is designed for use in IoT systems. It is based on the HTTP protocol and is intended for resource-constrained devices.

Frameworks:

- **AWS IoT:** Amazon Web Services (AWS) offers a range of tools and services for building and deploying IoT systems, including the AWS IoT platform. This platform provides a range of services, including device management, message broker, and data analytics.
- **Google Cloud IoT:** Google Cloud also offers a range of tools and services for building and deploying IoT systems, including the Google Cloud IoT platform. This platform provides a range of services, including device management, message broker, and data analytics.
- **Azure IoT:** Microsoft's Azure platform offers a range of tools and services for building and deploying IoT systems, including the Azure IoT platform. This platform provides a range of services, including device management, message broker, and data analytics.

Tools:

- **Arduino:** Arduino is an open-source electronics platform that is widely used for building and prototyping IoT systems. It includes a range of hardware and software tools, including a microcontroller, development environment, and libraries for connecting to sensors and other devices.
- **Raspberry Pi:** The Raspberry Pi is a small, low-cost computer that is widely used for building and prototyping IoT systems. It includes a range of hardware and software tools, including a microprocessor, operating system, and libraries for connecting to sensors and other devices.
- **Node-RED:** Node-RED is an open-source visual programming tool that is often used for building and prototyping IoT systems. It allows users to create flows using a drag-and-drop interface, making it easy to connect devices, sensors, and other components.

Hardware:

- **Sensors:** Sensors are an essential component of many IoT systems, and there are many different types of sensors available, including temperature sensors, humidity sensors, pressure sensors, and more.
- **Actuators:** Actuators are devices that can control physical systems, such as motors, valves, and pumps. They are often used in IoT systems to control and automate processes.
- **Gateway:** A gateway is a device that acts as a bridge between the physical world and the digital world. It is often used in IoT systems to connect sensors and actuators to a network or the internet.

APIs:

- **REST APIs:** REST (Representational State Transfer) APIs are a standard way of creating web-based APIs. They are often used in IoT systems to allow devices to communicate with each other and with other systems.
- **GraphQL APIs:** GraphQL is a query language that is used to create APIs. It allows clients to request specific data and is often used in IoT systems to allow devices to communicate with each other and with other systems.

Part 2

As an internet survey report, Analyze the impact of common IoT architecture, frameworks, tools, hardware and APIs in the software development life cycle.

IoT (Internet of Things) architecture refers to the overall design and structure of an IoT system. It involves selecting and combining various technologies and devices to create a cohesive system that can collect, transmit, and act on data from physical devices.

IoT frameworks are pre-designed sets of tools and protocols that provide a standardized way to develop and deploy IoT applications. They can help speed up the development process and ensure interoperability between different devices and systems.

IoT tools refer to the software programs and platforms that are used to build and manage IoT applications. These can include development tools, testing tools, and monitoring tools.

IoT hardware refers to the physical devices and sensors that make up an IoT system. This can include devices such as smart thermostats, connected light bulbs, and industrial machinery.

IoT APIs (Application Programming Interfaces) allow different devices and systems to communicate with each other and exchange data. They provide a standardized way for different components of an IoT system to communicate and integrate with each other.

In the software development life cycle, common IoT architecture, frameworks, tools, hardware, and APIs can have a significant impact. For example:

Internet of Things

- IoT architecture and frameworks can provide a foundation for the overall design of an IoT system and help ensure that it is scalable, secure, and reliable.
- IoT tools can streamline the development process and help developers build and test IoT applications more efficiently.
- IoT hardware can provide the necessary sensors and devices to collect and transmit data from the physical world.
- IoT APIs can enable different components of an IoT system to communicate and exchange data with each other, which is essential for the overall functionality of the system.

Overall, the use of common IoT architecture, frameworks, tools, hardware, and APIs can help make the development of IoT applications more efficient and effective, ultimately leading to better products and solutions for end users.

Part 4

Make some researches to evaluate above example scenario's (ADAS – emergency break) IOT architecture and justify their use when designing software applications.

Advanced Driver Assistance Systems (ADAS) use sensors and other technologies to assist drivers in various ways, including helping to prevent accidents by automatically applying the brakes in emergency situations. The Internet of Things (IoT) can play a role in the architecture of ADAS systems by providing a means of communication between the various sensors and devices involved in the system.

One key element of the IoT architecture for an ADAS emergency braking system is the use of sensors to detect potential hazards on the road. These sensors may include cameras, radar, and lidar, and they may be mounted on the vehicle itself or located at strategic points along the road. The sensor data is then transmitted to a central processing unit (CPU) via a wired or wireless connection.

The CPU uses this data to analyze the surrounding environment and make decisions about whether to initiate an emergency brake. If an emergency brake is deemed necessary, the CPU sends a signal to the brake system to activate the brakes.

The use of an IoT architecture in an ADAS emergency braking system has several advantages. One is that it allows for real-time communication between the sensors and the CPU, enabling the system to respond quickly to changing conditions on the road. Additionally, the use of sensors allows for a more comprehensive view of the surrounding environment, improving the accuracy of the system's decision-making.

Overall, the use of an IoT architecture in an ADAS emergency braking system can help to improve safety on the road by providing drivers with additional assistance in emergency situations.

Part 5

You currently work as a product developer for a new start up where you design IoT products for Transportation Industries. As part of your role your Project Manager has tasked you to plan and develop a new IoT product for potential client. You are required to identify a target user and conduct tests with this user and include this feedback into multiple iterative versions of your product. You can make testing using any toy vehicles.

Sure, I can help you with that! Here are the steps I recommend you take to plan and develop a new IoT product for transportation industries:

1. Identify your target user: Who will be using your product? What are their needs and goals? Understanding your target user will help you design a product that meets their needs and addresses their pain points.
2. Conduct market research: Look for similar products on the market and see what users like and dislike about them. This will help you understand what features are important to your target user and how you can differentiate your product from the competition.
3. Define your product: Based on your research and understanding of your target user, create a detailed product specification that outlines the features, functionality, and design of your product.
4. Prototype and test: Create a prototype of your product using toy vehicles or other materials. This will allow you to test the functionality and user experience of your product.
5. Iterate and refine: Based on feedback from your testing, make changes to your prototype and continue testing until you have a product that meets the needs of your target user.
6. Launch and market: Once your product is ready, it's time to launch it and start marketing it to potential customers. This may involve creating marketing materials, setting up a sales channel, and promoting your product through various channels.

Plan an IoT application for a specific target end user and the tests you intend to conduct with this user. This plan will be in the form of a document and will include supporting evidence and material, such as user personas and customer journey maps.

IoT Application: Smart Home Security System

Target End User: Homeowners with young children

User Personas:

- Maria is a 35-year-old stay-at-home mom with two young children. She is always worried about the safety of her kids and is looking for ways to secure her home.
- John is a 40-year-old working professional who travels frequently for work. He is concerned about the security of his home while he is away and wants to be able to monitor his home remotely.

Customer Journey Map:

1. Maria and John both become aware of the smart home security system through online research or word-of-mouth from friends.
2. They visit the company's website to learn more about the product and its features.
3. Maria and John decide to purchase the system and have it installed in their homes.
4. They download the app and set up their account, connecting all of the devices in their home.
5. Maria and John are now able to monitor their homes remotely and receive alerts if any unusual activity is detected.

Tests:

1. User experience: We will ask Maria and John to use the system for a week and provide feedback on the ease of use and overall user experience.
2. Security: We will conduct penetration testing to ensure that the system is secure and not vulnerable to hacking.
3. Alert accuracy: We will set up various scenarios (e.g. a door opening, a window breaking) and monitor the system's response to ensure that it is accurately detecting and alerting the user of potential security threats.
4. Remote monitoring: We will have John remotely monitor his home from a different location to ensure that he is able to access the live feed and receive alerts as intended.

Create multiple iterations of your application and modify each iteration with enhancements gathered from user feedback and experimentation. This will follow the pathway outlined in your plan.

Sure! Here is a general outline of the process for creating multiple iterations of an application and incorporating enhancements based on user feedback and experimentation:

1. Develop the initial version of your application according to your plan.
2. Release the application and gather feedback from users. This can be done through surveys, user testing, or other methods.
3. Analyze the feedback and identify common themes or issues.
4. Based on the feedback, create a list of enhancements or changes that you would like to make to the application.
5. Prioritize the list of enhancements and select those that will be included in the next iteration of the application.
6. Develop the next iteration of the application, incorporating the selected enhancements.
7. Repeat the process of gathering feedback, analyzing it, and making enhancements until you have reached the desired level of quality and functionality for the application.

It's important to note that this process should be ongoing and iterative, as you will continue to gather feedback and make enhancements throughout the lifetime of the application.

Conclusion

A conclusion is a summary of the main points of your assignment and should demonstrate to the reader that you have achieved a good understanding of the topic. Some key things to include in a conclusion for an IoT assignment could be:

1. A summary of the main points you have covered in your assignment, including the key technologies and concepts you have discussed.
2. A discussion of the implications of IoT technology and how it is likely to impact society and industry in the future.
3. An evaluation of the potential benefits and drawbacks of IoT, including any ethical or privacy concerns that may arise.
4. Some possible directions for future research in the field of IoT.

Remember to keep your conclusion brief and to the point, and to avoid introducing any new information that has not been covered in your assignment.

Reference

<https://assignmentpoint.com/internet-of-things-iot/>

<https://desklib.com/document/iot-iot-internet-of-things-abstract/>

<https://www.studocu.com/row/document/addis-ababa-science-and-technology-university/computer-science/iot-assignment-good/30562243>

<https://www.scribd.com/document/443878269/IOT-assignment>

<https://dl.acm.org/doi/abs/10.5555/3344013.3344032>

<https://www.tes.com/teaching-resource/the-internet-of-things-iot-bundle-assignments-1-2-12338143>

<https://www.sciencedirect.com/science/article/abs/pii/S138912862200189X>

<https://ieeexplore.ieee.org/document/9764088>